EMPLOYMENT OPPORTUNITY ANNOUNCEMENT

DEPARTMENTS OF THE ARMY AND AIR FORCE
OFFICE OF THE ADJUTANT GENERAL
NORTH CAROLINA NATIONAL GUARD
HUMAN RESOURCES OFFICE
4105 REEDY CREEK ROAD
RALEIGH, NORTH CAROLINA 27607-6410

ANNOUNCEMENT #: ANG 11-2004

OPENING DATE: 06 February 2004
CLOSING DATE: 08 March 2004

ANTICIPATED FILL DATE: 04 April 2004

POSITION TITLE AND NUMBER:

Information Technology Specialist (INFOSEC)
PDCN: F80465000

UNIT/ACTIVITY AND DUTY LOCATION:

263rd Combat Communications Squadron, NCANG, Badin, NC

GRADE AND SALARY:

TECH

GS-2210-11 $47,110 - $61,248 per annum

EMPLOYMENT STATUS:

Excepted Service

WHO CAN APPLY: The area of consideration for this position is Statewide. Applications will only be accepted from current Excepted employees of the North Carolina Air National Guard.

HOW TO APPLY: TECHNICIAN: Applicants interested in the technician position may apply by submitting an Optional Application for Federal Employment (Optional Form 612), resume or any other form of application. It is required that the Knowledge, Skills and Abilities (KSA) listed below be addressed and attached to the application. **NOTE: Information that must be provided when applying for a technician position is as follows: announcement number; name; address; telephone number; social security number; date of birth; citizenship; education; work experience; and other job-related qualifications.**

Applications must be sent to: North Carolina National Guard, ATTN: OTAGNC-HRO, 4105 Reedy Creek Road, Raleigh, NC 27607-6410, to be received not later than the close of business on the above indicated closing date.

QUALIFICATION REQUIREMENT: TECHNICIAN: Must have 36 months specialized experience which demonstrates the applicant has acquired the below listed KSA'S.

KNOWLEDGE, SKILLS & ABILITIES (KSA'S)

Below are listed the KSA's for this position. Each technician applicant must address each KSA individually in paragraph format by explaining any civilian and military work experience (with dates) that provided that KSA. These comments must be addressed in the order they appear below and attached to the application when applying for the position. Failure to include attachment of the KSA Statement will result in your application not being considered for employment. ASSISTANCE IN COMPLETING THE KSA STATEMENT MAY BE OBTAINED BY CALLING OR 704/391-4169.

1. Ability to research and analyze data.
2. Ability to communicate orally and in writing.
3. Skill in organizing work in a logical sequence.
4. Knowledge of a wide range of communications security, techniques, requirements, methods, sources and procedures for the following programs: Communications Security (COMSEC), Cryptographic Access Program (CAP), Electronic Key Management System (AFEKMS), STU III, FORTEZZA security and Security Awareness, Training and Education (SATE).
5. Knowledge of a wide variety of communications security concepts, principles, practices and governing directives to interpret, disseminate and adapt local policy and implement instructions to unit personnel.

CONDITION OF EMPLOYMENT: Occupants of this position must maintain continuous military membership in the North Carolina Air National Guard (NCANG). NCANG status (military grade, DAFSC, military unit) and experience must be entered on the application. The recommended applicant will not be approved for appointment until they occupy a compatible AFSC in the NCANG shown under Military Assignment on the reverse side of this announcement. The applicant selected for this position will be required to participate in the Direct Deposit/Electronic Fund Transfer Program. The recommended applicant will not be approved for promotion/appointment until the appropriate physical examination is completed.

MILITARY ASSIGNMENT: Assignment in a compatible Enlisted position in the NCANG. AGR GRADE: not to exceed CMSGT/E-9. AFSC: 3C0X1, 3C2X1, 2E2X1

EVALUATION FACTORS USED: Personal interviews, review of application and the KSA Statement.

PRINCIPAL DUTIES AND RESPONSIBILITIES:

Serves as the Computer Security (COMPUSEC) Manager. Protects and maintains the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. Establishes and publishes squadron policy to manage the COMPUSEC program. Disseminates information and ensures computer security practices are adhered to by all functional areas in-garrison and in support of deployed war-fighting personnel. Reviews, analyzes, and validates certification and accreditation packages. Continuously identifies and analyzes threats and vulnerabilities to the information systems to maintain an appropriate level of protection. Ensures computer software designs address information system security requirements. Accomplishes risk analysis, security testing, and certification due to modifications or changes to computer systems. Evaluates, assesses, or locally tests and approves all hardware, software, and firmware products that provide security features prior to use on any accredited information system or network. Certifies all software prior to installation and use on communications and computer systems. Executes computer security plans and enforces mandatory access control techniques such as trusted routers, bastion hosts, gateways, firewalls, or other methods of information systems protection. Manages the Information Assurance Program. Implements procedures to ensure protection of information transmitted to the squadron, among units in the squadron, and from the squadron units using local or wide area networks, the worldwide web or other communications modes. Utilizes current and future multi-level security products collectively to provide data integrity, confidentiality, authentication, non-repudiation, and access control of the Local Area Network (LAN). Reports to Major Command (MAJCOM), Air Force Communications Agency (AFCA), National Security Agency (NSA), and Air Force Computer Emergency Response Team (AFCERT) all incidents involving viruses, tampering, or unauthorized system entry. Controls access to prevent unauthorized persons from using network facilities. Limits access to privileged programs (i.e., operating system, system parameter and configuration files, and databases), utilities, and security-relevant programs/data files to authorized personnel. Implements methods to prevent or minimize direct access, electronic or other forms of eavesdropping, interpreting electro-mechanical emanations, electronic intercept, telemetry interpretation, and other techniques designed to gain unauthorized access to Automated Data Processing (ADP) information, equipment, or processes. Recognizes such potential and defines vulnerabilities and oversees the installation of physical and technical security barriers to prevent others from improperly obtaining such information. Serves as the Communications Security (COMSEC) Manager for all cryptographic activities including managing the Cryptographic Access Program (CAP). Formulates and develops communications security criteria and requirements for inclusion in mobility, contingency, and exercise plans. Maintains accountability for sensitive cryptographic materials and related COMSEC information. Oversees issuance of COMSEC materials. Maintains COMSEC inventory on the Computerized Management of COMSEC Material (CM2) database. Prepares and evaluates written plans for emergency actions and ensures personnel are fully qualified in the execution of plans. Investigates security incidents to determine the possibility of compromise to COMSEC materials and ensures documentation and reporting to appropriate channels. Performs destruction, receiving, issuing, and inspecting COMSEC material within the most stringent timelines. Furnishes written guidance to user accounts concurring effective dates, accounting procedures, destruction requirements, and physical security of COMSEC keying materials. Performs semi-annual functional reviews of all COMSEC user accounts, physically inspecting the user's COMSEC facilities, reviewing procedures, and audit of all cryptographic holdings. As required, manages the Certification Authority Workstation. Administers the CAP by conducting briefings prior to granting access to cryptographic information. Documents cryptographic access certificates and acts as liaison for scheduling polygraph examinations of personnel

enrolled in the program. Implements and manages the Air Force Electronic Key Management System program. This includes system configuration and operation of the Local Management Device, Data Transfer Device, and Key Processor. Initializes the system, performs system backups, determines operator access, and control functions (privilege management), reloads and configures the operating system's parameters. Installs or oversees installation of local COMSEC account hardware and software, including training alternates in the AFEKMS operations. Serves as secure telecommunications units/elements (STU-III) representative and Emissions Security Program (EMSEC) administrator. Develops, implements, and monitors security systems for the protection of controlled cryptographic cards, documents, ciphers, devices, communications centers, and equipment. Validates strapping and configuration options of cryptographic units. Provides technical training and instruction on Computer Security Awareness Training and Education (SATE) program procedures to supervisors, employees, and/or unit security representatives. Utilizes computer-based training for both initial and recurring information protection training. Conveys the degree of reliance on information systems, the potential consequences arising from the lack of secure information systems, the organization's commitment to secure information systems, and the means by which users can protect information systems. Conducts annual COMSEC training for squadron COMSEC users. Uses a wide variety of formal training materials, such as outlines, handouts, publications, films, exhibits, protective devices, and visual aids to provide and/or reinforce information related to communications-computer systems security awareness practices. Promotes security campaigns through oral presentations at local security committee meetings; and extracts, compiles, and prepares security articles, bulletins, and pamphlets for local use by squadron personnel. Maintains required course records. Assists unit personnel with duties involving a wide range of communications and information systems and telecommunications programs consisting of tactical communications equipment, LAN systems, information resource management, and information protection programs. Performs other duties as assigned,

INSTRUCTIONS TO COMMANDERS/SUPERVISORS: This position vacancy announcement will be given the broadest possible dissemination. A copy of this announcement will be posted to your unit/activity bulletin board. A copy of this announcement will be posted to the 145 MSF web page.

ADDITIONAL INSTRUCTIONS:

1. Applicants are requested to identify, on a separate sheet of paper, their race and national origin from one of the following categories: Male or female; American Indian or Alaskan native; Asian or Pacific Islander; Black, not of Hispanic origin; Hispanic; white, not of Hispanic origin. Submission of this information is voluntary and will be used in support of the NCNG Equal Employment and Affirmative Action Programs.
2. An initial, and periodic medical examination may be required for jobs located in working areas which have a high exposure risk to conditions which may result in occupational illness or injury.
3. Participants in the Selected Reserve Incentive Program will be administered as prescribed by NGB Pamphlet 600-15.
4. A permanent change of station (PCS) will not be authorized for the individual selected for this position unless agreed upon in advance by HRO and a PCS order is prepared prior to effective date.
5. Males born on or after 1 January 1960 must be registered with the Selective Service in order to be considered for federal employment.

DISTRIBUTION:
A, B-3, C-3, G-25, H-3, J-3, K-3, M, N-12, P-9, Q, W-2, Y-2, R: HRO-20, AGAV-1, AGCS-3, DCSANG-1, DCSLOG/G4-4, DCSOI-3, DCSPER-3, FMCB-2, IG-1, SCSM-1, SRAA-1, VCSOP-1